UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,429	03/13/2006	David Arditti Modiano	0600-1192	8849

466 7590 12/30/2008
YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
ARCHER, CHRISTOPHER B	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
12/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/560,429	ARDITTI MODIANO ET AL.	
	Examiner	Art Unit	
	CHRISTOPHER B. ARCHER	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-18 and 27-35* is/are rejected.

7)☒ Claim(s) *19-26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *14 December 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/560,429 filed on 03/13/2006 is presented for examination by the examiner.

Examiner Notes

2. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Oath/Declaration

3. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Priority

4. As required bye **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on June 17, 2003 (FR 0307287).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/14/2005 is being considered by the examiner.

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino

acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Objections

6. Claim 19 is objected to because of the following informalities:

In regards to the equation "$1 + q^{o1} + \ldots + q^{o1} + \ldots + q^{od-1}$," the second instance of q^{o1} appears to be a typo. In accordance with the specifications, page 4, line 13, the examiner read this statement as "$1 + q^{o1} + \ldots + q^{oi} + \ldots + q^{od-1}$."

Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 27, 28, and 31-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because of the following reason:

The claims fails to place the invention squarely within one statutory class of invention. The applicant has not provided evidence that applicant does not intend the "medium" to include signals. As such, the claims are drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim(s) is/are not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a composition of matter.

Claim 30 is rejected under 35 U.S.C. 101 as non-statutory for at least the reason stated above. Claim 30 is depended on claim 28, however, it do not add any feature or subject matter that would solve any of the non-statutory deficiencies of claim 28.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 18 recites the limitation "said mathematical description (F_{kj})." There is insufficient antecedent basis for this limitation in the claim.

For the purposes of examination, the examiner will consider "said mathematical description (F_{kj})" to refer to the "mathematical description of the decoder" as mentioned in claim 17.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 16, 18, 27, 28, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. "An Efficient Public Key Traitor Tracing Scheme" *Advances in Cryptology – Crypto '99. 19th Annual International Cryptology Conference Proceedings.* Santa Barbara, CA, USA (1999) pages 338-353, hereafter referred to as Boneh, in view of "Public Quadratic

Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption." *Advances In Cryptology- Eurocrypt '88. International Conference on the Theory and Application of Cryptographic Techniques Proceedings.* Springer Verlag, DE (1988), pages 419-453, hereafter referred to as Matsumoto.

Regarding claim 16:

Boneh discloses:

"Traceable method for encrypting and/or decrypting data broadcast by at least one transmitter towards several decoders, this method enabling the identification of a traitor, amongst different lawful users of the decoders, who has communicated secret data to a non-authorized third party so that this third party is able to encrypt and/or decrypt data broadcast by the transmitter, in which:

- during encryption of the broadcast data, the transmitter applies at least a first secret cryptographic function, and

wherein during the application of the second function the mathematical description of this second function, to which each decoder has recourse, is different from one decoder to another or from one group of decoders to another so that the mathematical description to which recourse is made exclusively identifies the particular decoder or group of decoders among all the decoders."

[(Boneh pages 338-339, Introduction ¶ 1-3) shows a digital content distribution system involving distributors and subscribers. In this system, each subscriber or group of subscribers are given a distinct, identifying set of keys. These keys can be symmetric or asymmetric in nature.]

But Boneh fails to explicitly disclose:

"during decryption of said broadcast data, all the decoders apply at least one same second secret cryptographic function identical to said first function or its inverse, each decoder having recourse for this purpose to a mathematical description of said second function recorded in a memory."

However, Matsumoto discloses:

"during decryption of said broadcast data, all the decoders apply at least one same second secret cryptographic function identical to said first function or its inverse, each decoder having recourse for this purpose to a mathematical description of said second function recorded in a memory."

[(Matsumoto page 422, S2-1) shows that each polynomial equation is an affine bijection. (Matsumoto page 422, S3) shows that each key is composed of a series of functions.]

Boneh and Matsumoto are analogous art because they are from the same field of endeavor of key encryption, decryption, and creation, as well as traitor-tracing.

It would have been obvious to one of ordinary skill in the art at the time of the invention to improve Boneh's invention by using the public key scheme of Matsumoto to encrypt and decrypt digital content as Matsumoto's scheme reduces the computational complexity of public-key cryptography.

Regarding claim 18:

Matsumoto further discloses:

"Method as in claim 16, wherein said mathematical description (F_{Kj}) recorded in the memory of each decoder is formed of several elementary functions (G_{ij}) which must be composed with each other in a determined order to form said second secret function."

[(Matsumoto page 422) shows that each key is composed of a series of functions in a predetermined order.]

Regarding claim 27:

Boneh further discloses:

"Data recording medium, wherein it comprises instructions for the execution of a traceable encryption and/or decryption method according to claim 16, when these instructions are executed by a decoder."

[(Boneh pages 338-339, Introduction ¶ 1-3) shows the keys being stored in and used by a receiver.]

Regarding claim 28:

Boneh further discloses:

"Data recording medium, wherein it comprises instructions for the execution of a traceable data encryption and/or decryption method as in claim 16, when said instructions are executed by a transmitter."

[(Boneh pages 338-339, Introduction ¶ 1-3) shows the keys being stored in and used by a distributor to encrypt data before the data is sent to a corresponding receiver.]

Regarding claim 32:

Boneh further discloses:

"Data recording medium, wherein it comprises instructions for the execution of a traceable data encryption and/or decryption method as in claim 18, when said instructions are executed by a transmitter."

[(Boneh pages 338-339, Introduction ¶ 1-3) shows the keys being stored in and used by a distributor to encrypt data before the data is sent to a corresponding receiver.]

12. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh in view of Matsumoto.

Regarding claim 29:

Boneh discloses:

"Traceable system for encrypting and/or decrypting broadcast data capable of identifying a traitor, among different lawful users, who has communicated secret data to a non-authorized third party so that this third party is able to encrypt and/or decrypt the broadcast data, this system comprising:

- a transmitter able to encrypt broadcast data, this transmitter being capable of applying at least a first secret cryptographic function, to directly process a message, then of broadcasting the message,

- several decoders able to decrypt broadcast data

wherein the memory of each decoder contains a mathematical description of said second function different from the one recorded in the memory of the other decoders or in the memory of the other groups of decoders so that this mathematical description exclusively identifies the particular decoder or group of decoders among all the decoders."

[(Boneh pages 338-339, Introduction ¶ 1-3) shows a digital content distribution system involving distributors and subscribers. In this system, each subscriber or group of subscribers are given a distinct, identifying set of keys. These keys can be symmetric or asymmetric in nature.]

But Boneh fails to explicitly disclose:

"all the decoders being able to apply a second secret cryptographic function identical to said first function or to its inverse for the direct processing of said broadcast message, each decoder for this purpose being equipped with a memory in which a mathematical description of said second function is recorded."

However, Matsumoto discloses:

"all the decoders being able to apply a second secret cryptographic function identical to said first function or to its inverse for the direct processing of said broadcast message, each decoder for this purpose being equipped with a memory in which a mathematical description of said second function is recorded."

[(Matsumoto page 422, S2-1) shows that each polynomial equation is an affine bijection. (Matsumoto page 422, S3) shows that each key is composed of a series of functions.]

Boneh and Matsumoto are analogous art because they are from the same field of endeavor of key encryption, decryption, and creation, as well as traitor-tracing.

It would have been obvious to one of ordinary skill in the art at the time of the invention to improve Boneh's invention by using the public key scheme of Matsumoto to encrypt and decrypt digital content as Matsumoto's scheme reduces the computational complexity of public-key cryptography.

13. Claims 17 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh in view of Matsumoto and further in view of Gazier et al. (U.S. Patent No. 6,880,088), hereafter referred to as Gazier.

Regarding claim 17:

Boneh and Matsumoto disclose:

"Method as in claim 16," but fail to explicitly disclose: "wherein the second cryptographic function is able to process non-redundant data."

However, Gazier discloses:

"Wherein the second cryptographic function is able to process non-redundant data."

[(Gazier column 2, lines 57-59) shows that it is common for secure communication networks to process non-redundant data.]

Gazier and Boneh are analogous art because they are from the same field of endeavor of secure digital data communication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to improve the invention of Boneh by allowing the invention to process non-redundant data, as disclosed in the invention of Gaizer, in order to allow for the conservation of bandwidth.

Regarding claim 31:

Boneh further discloses:

"Data recording medium, wherein it comprises instructions for the execution of a traceable data encryption and/or decryption method as in claim 17, when said instructions are executed by a transmitter."

[(Boneh pages 338-339, Introduction ¶ 1-3) shows the keys being stored in and used by a distributor to encrypt data before the data is sent to a corresponding receiver.]

Allowable Subject Matter

14. Claims 19-26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER B. ARCHER whose telephone number is (571)270-7308. The examiner can normally be reached on M-F 7:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER B ARCHER/
Examiner, Art Unit 4148

/THOMAS K PHAM/
Supervisory Patent Examiner, Art Unit 4148